

JAQUELINE MARTINS DINIZ

**AUDITORIA INTERNA:
ANÁLISE DOS PROCESSOS INTERNOS E DOS RISCOS OPERACIONAIS**

Monografia apresentada ao Programa do Curso de Pós-Graduação do Departamento de Contabilidade do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, como requisito para obtenção do título de especialista em Gestão de Negócios – turma 2009.

Professor Orientador: MSc. Wesley Souza do Nascimento

**CURITIBA
2010**

**Este trabalho é dedicado aos
profissionais da educação que, apesar
de todas as dificuldades, acreditam
que esta é a mola mestra para o
desenvolvimento humano e por isso
nunca desistem.**

AGRADECIMENTOS

Aos professores da graduação e da Pós Graduação da UFPR, que muito contribuíram para o meu desenvolvimento profissional e acadêmico.

A todas as pessoas que fizeram ou fazem parte da minha vida e cuja amizade é incondicional.

A minha mãe, irmãs e sobrinhos, pessoas que sempre me apoiaram e souberam me entender nos momentos difíceis.

E o meu agradecimento mais do que especial à Jaqueline Kugler Tibucheski, professora dedicada e entusiasta pela educação, fiel aos seus princípios e ideais educacionais que, com seu apoio e incentivo, foi a principal responsável por eu ter chegado até aqui. A você, minha gratidão eterna.

RESUMO

DINIZ, Jaqueline Martins. Por ser a auditoria interna uma poderosa ferramenta de controle sobre as informações, registros, ações e atividades existentes nas organizações. Serve de auxílio aos administradores/proprietários na tomada de decisão, no controle efetivo da organização e verificação de fraudes e/ou incorreções. Tem em seus relatórios, recomendações e comentários; a fonte para a obtenção de importantes e relevantes informações. Assim sendo, o setor administrativo de auditoria interna deve ser implementado nas organizações que, assim como o mercado, estão em constante desenvolvimento. O auditor interno, cujo trabalho objetiva o aprimoramento dos controles, redução dos custos e melhoria nos produtos, em muito se assemelha ao auditor externo. A diferença básica entre eles é a forma de atuação, enquanto o primeiro atende às necessidades da administração, o segundo atende às necessidades de terceiros no que diz respeito à fidedignidade das informações financeiras. Neste sentido, o auditor externo possui menos tempo hábil para uma efetiva e profunda análise dos controles e procedimentos da organização, fazendo com que seja necessária a figura do auditor interno. Uma vez que esta função poderá ser exercida por um funcionário da organização, este estará mais próximo e presente no acompanhamento das atividades diárias e na identificação de possíveis problemas. As análises dos riscos e atividades devem ser realizadas por profissional que possua algum tipo de envolvimento mais direto com a organização, o que facilita a coleta de informações e o acesso aos diversos setores existentes. Precisa possuir também bom conhecimento do negócio da organização, para que, ao receber as informações, saiba em que momento elas se entrelaçam na *network* existente e qual o reflexo gerado.

Palavras-chave: controles internos; riscos; estratégia; Governança Corporativa

SUMÁRIO

DEDICATÓRIA..... ii

AGRADECIMENTOS iii

RESUMO..... iv

1 INTRODUÇÃO 1

1.1 Considerações Iniciais..... 1

1.2 Objetivos 2

1.2.1 Geral..... 2

1.2.2 Específicos 2

2 AUDITORIA EXTERNA X INTERNA..... 3

3 CONTROLES INTERNOS..... 6

3.1 Self Assessment (CSA) 7

3.2 COSO 10

3.3 COBIT 15

4 AUDITORIA INTERNA E A GOVERNANÇA CORPORATIVA..... 20

5 IMPLANTANDO A ÁREA DE AUDITORIA INTERNA 23

5.1 Estruturação da Auditoria Interna..... 24

5.2 Elaboração do Plano de Auditoria Interna 25

5.3 Execução do Plano de Auditoria Interna 28

6 CONCLUSÃO..... 30

REFERÊNCIAS..... 31

1 INTRODUÇÃO

1.1 Considerações Iniciais

Com a expansão cada vez maior das empresas, seja pela inauguração de novas filiais ou pela diversificação e aumento da produção, essas adquirem novos compromissos e contratam mais funcionários. Novas aquisições geram a necessidade de que as estratégias gerenciais sejam corretamente implementadas e executadas.

Tendo em vista a impossibilidade dos gestores acompanharem pessoalmente todas as atividades existentes numa organização, avaliando se as normas e os procedimentos internos estariam sendo observados por todos, viu-se a necessidade da criação de uma função específica no organograma que desse suporte aos gestores. Nesse sentido, surgiu a auditoria interna com a função de acompanhamento e gerenciamento dos processos produtivos e sua efetiva execução, bem como a análise dos riscos envolvidos na operação da empresa, salvaguardando seus ativos.

O trabalho do auditor interno está relacionado ao entendimento do negócio, a montagem do cenário operacional, estruturação dos controles internos, análise de riscos operacionais e análise dos resultados apresentados. A função administrativa auditoria necessita também do auxílio de outras três funções: o planejamento, a execução e o controle. Portanto, o auditor interno deve ser um profissional com conhecimentos contábeis e com bom relacionamento interpessoal, o que lhe facilita a obtenção das informações necessárias para a realização de suas tarefas.

Com a publicação da Lei Sarbanes-Oxley (SOX), em 2002 pelo governo norte-americano, as empresas que pretendem obter recursos no mercado de capitais ou acessar mercados internacionais, precisam obter a conformidade com a Seção 204 que menciona ser necessária a revisão da forma pela qual são realizados os principais processos de negócio.

Para auxiliar o auditor interno nesta tarefa dois modelos de gestão, sugeridos pela SEC (*Securities and Exchange Commission*), órgão norte-americano responsável pela implantação da SOX, precisam ser aplicados: o *Framework COSO (Committee of Sponsoring Organizations of Treadway Commission)* para a gestão de riscos dos

negócios e o *Framework COBIT (Control Objectives for Information and related Technology)* para atender aos requisitos de controle dos processos de tecnologia da informação. Além destes encontramos também o Control Self Assessment (CSA).

No dia-a-dia de uma organização, muitos dados são recebidos e tratados dentro dos diversos setores da organização. Porém, para que o seu crescimento seja confiável e sólido essas informações precisam ser analisadas e encaminhadas aos gestores em tempo real, permitindo assim uma tomada de decisão mais rápida. Além dos gestores, todos os colaboradores precisam de um *feedback* no que diz respeito às suas atividades, o que permite um maior entendimento quanto à relevância e importância das informações a serem compartilhadas pelos setores e dos riscos envolvidos.

Neste trabalho serão apresentadas ferramentas e procedimentos de auditoria que viabilizam o auxílio na melhoria da geração de informações e na análise dos riscos, assim como o compartilhamento das mesmas, com o objetivo de que o resultado operacional da organização seja sempre melhorado e os riscos mitigados.

1.2 Objetivos

1.2.1 Geral

O objetivo geral deste trabalho é apresentar ferramentas para o auxílio ao gestor na tomada de decisão e indicar os melhores métodos para o acompanhamento das atividades operacionais da organização, onde se encontram os controles internos e os sistemas de tecnologia da informação que promovam uma maior integração da organização, na busca de melhores resultados.

1.2.2 Específicos

Como objetivos específicos destacam-se:

- Demonstrar a necessidade da existência do setor de auditoria interna nas empresas, suportando a tomada de decisão dos gestores.
- Definir os pontos relevantes a serem observados pela auditoria interna.
- Apresentar os métodos a serem utilizados pelo setor.
- Descrever algumas das ferramentas mais utilizadas para auxílio no desenvolvimento dos trabalhos.

2 AUDITORIA EXTERNA X INTERNA

Conforme Almeida (2003, p. 25) “A auditoria externa ou auditoria independente surgiu como parte da evolução do sistema capitalista”.

Com o crescimento das instalações fabris e o acirramento da concorrência foi necessário o aprimoramento dos controles e procedimentos internos, visando, principalmente, a redução dos custos. Para que todas essas mudanças fossem possíveis, as organizações passaram a recorrer às instituições financeiras, ou a abertura de capital, à procura de recursos. Para a efetivação destes empréstimos, os futuros investidores precisavam conhecer como estava sendo conduzida a administração financeira destas empresas, através da sua posição patrimonial e financeira, apresentada nas Demonstrações Financeiras.

Como medida de segurança contra manipulação de informações, os investidores começaram a exigir a existência de um parecer de profissional independente, que garantisse a veracidade das informações contidas nessas Demonstrações. Além do parecer, o auditor externo começou a apresentar um relatório-comentário, onde sugestões eram apresentadas a cerca de problemas que chegavam ao seu conhecimento durante a execução de seu trabalho.

Na tentativa de minimizar estes problemas e não podendo contar com o auditor externo, uma vez que este permanece na empresa por um período de tempo muito curto, Almeida (2003, p. 29) comenta: “Para atender a Administração da empresa, seria necessária uma auditoria mais periódica, com maior grau de profundidade e visando também as outras áreas não relacionadas com contabilidade (sistema de controle de qualidade, administração de pessoal etc.)”.

Surgiu então, a figura do auditor interno, contador, funcionário da empresa, sem subordinação àqueles aos quais irá executar seus exames ou desenvolver qualquer atividade que interfira na sua independência. O profissional auditor interno tem como atos regulatórios para o exercício de suas funções a Resolução CFC 781/1995 que aprovou a NBC-P-3 - Normas Profissionais de Auditor Interno e a Resolução CFC 986/2003 que aprovou a NBC-T-12 - Normas Técnicas de Auditoria Interna. Além destas Resoluções, este profissional deve se basear no padrão internacional estabelecido para o Auditor Independente (NBC-TA), bem como o Código de Ética do Contabilista baixado pela Resolução CFC 803/1996.

Conforme Imoniana (2001, p. 35) “A filosofia desta profissão tem se baseado no seguinte: a) Evidência; b) Diligência e Cuidados; c) Fidedignidade da Apresentação e, e) Ética Profissional”.

A seguir, a estrutura organizacional (Figura 1), demonstrando a posição a ser ocupada pela Auditoria:

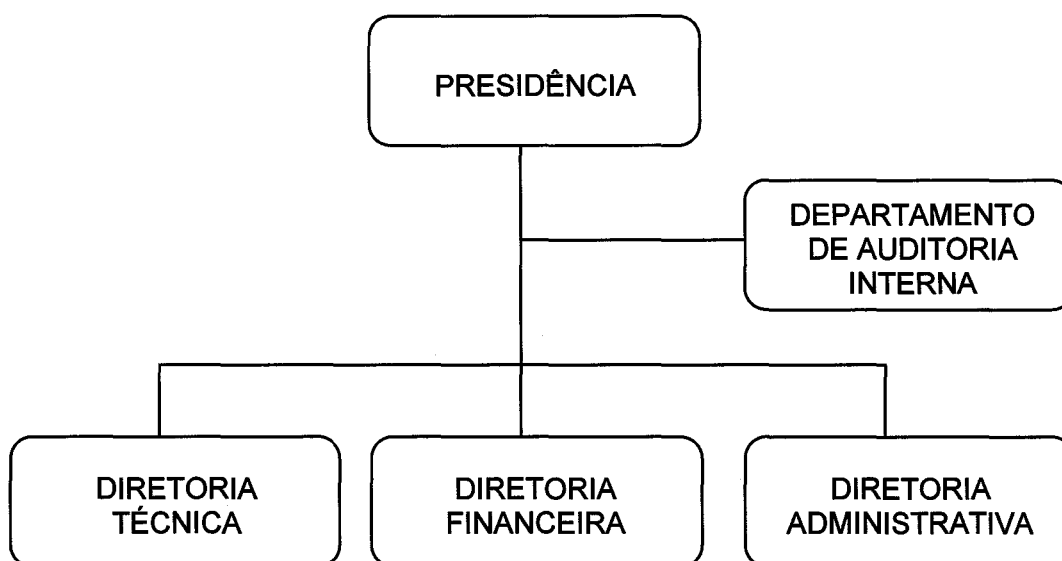


Figura 1 – Estrutura organizacional

Fonte: Almeida, 2003, p. 30.

Segundo Gil (2002, p.112):

“A função administrativa auditoria, para seu correto e adequado exercício, necessita de metodologia ágil e com princípios sintonizados ao ambiente dos negócios, o qual tem como fundamentos:

- Intensas e constantes mudanças de mercado e de sua tecnologia agregada;
- Elevado volume de transações em processamento;
- Alta velocidade do processamento das transações;
- Forte capacidade de integração operacional para disponibilizar informações necessárias ao funcionamento e tomada de decisão do negócio;
- Grande diversidade de tarefas e informações componentes das linhas de negócios.”

O auditor interno não tem como foco as análises dos resultados apresentados nas demonstrações financeiras geradas, mas sim a eficácia dos controles internos e dos riscos gerados durante a operação da organização, conforme apresentado no Quadro 1.

Quadro 1 - Comparativo Atividades Auditoria

<u>Auditoria Interna</u>	<u>Auditoria Externa</u>
A auditoria pode ser realizada por um funcionário da empresa	A auditoria é realizada através de contratação de um profissional independente
O objetivo principal é atender as necessidades da administração	O objetivo principal é atender as necessidades de terceiros no que diz respeito à fidedignidade das informações financeiras
A revisão das operações e do controle interno é principalmente realizada para desenvolver aperfeiçoamento e para induzir ao cumprimento de políticas e normas, sem estar restrito aos assuntos financeiros	A revisão das operações e do controle interno é principalmente realizada para determinar a extensão do exame e a fidedignidade das demonstrações financeiras
O trabalho é subdividido em relação às áreas operacionais e às linhas de responsabilidade administrativa	O trabalho é subdividido em relação às contas do balanço patrimonial e da demonstração do resultado
O auditor diretamente se preocupa com a detecção e prevenção de fraude	O auditor incidentalmente se preocupa com a detecção e prevenção de fraudes, a não ser que haja possibilidade de substancialmente afetar as demonstrações financeiras
O auditor deve ser independente em relação às pessoas cujo trabalho ele examina, porém subordinado às necessidades e desejos da alta administração	O auditor deve ser independente em relação à administração, de fato e de atitude mental
A revisão das atividades da empresa é contínua	O exame das informações comprobatórias das demonstrações financeiras é periódica, geralmente semestral ou anual.

Fonte: Em Portal Educação – Maph Editora

Conforme o quadro acima, através do mapeamento dos processos e validação dos controles e processos existentes na organização, a Auditoria Interna procura certificar-se de que as normas e diretrizes da organização estão sendo cumpridas, permitindo assim que o objetivo traçado pela alta administração seja alcançado, não dando tanta ênfase aos resultados financeiros. Não significando que a Auditoria Interna os ignore, eles também fazem parte do escopo de trabalho da Auditoria Interna. O resultado financeiro de uma organização deve ser analisado e validado pelos Auditores Externos, através de seus pareceres, atendendo assim as exigências estabelecidas pelos fornecedores externos da organização.

3 CONTROLES INTERNOS

Almeida (2003, p. 63) define o controle interno:

“[...] conjunto de procedimentos, métodos ou rotinas com os objetivos de proteger os ativos, produzir dados contábeis confiáveis e ajudar a administração na condução ordenada dos negócios da empresa.”

Imoniana (2001, p. 93) comenta:

“[...] nenhuma pessoa será responsável por uma só operação desde o seu princípio até o seu fim. Para ajudar nesta tarefa tediosa, criaram-se controles internos eficazes e necessários para proteger os bens e evitar as fraudes.”

A simples existência dos controles internos não garante que a organização esteja imune a fraudes ou inconsistências sistêmicas, por isto a auditoria interna necessita verificar seus pontos vulneráveis, assim definidos pela metodologia COSO:

- **custo/benefício:** todo controle tem um custo, que deve ser inferior à perda decorrente da consumação do risco controlado;
- **conluio entre empregados:** da mesma maneira que as pessoas são responsáveis pelos controles, estas pessoas podem valer-se de seus conhecimentos e competências para burlar os controles, com objetivos ilícitos.
- **eventos externos:** eventos externos estão além do controle de qualquer organização.

O levantamento do sistema de controle interno pode ser obtido através de leitura de manuais, conversa com funcionários ou inspeção física desde o início da operação até seu final. Estas informações devem ser registradas em memorandos narrativos, questionários padrões ou fluxogramas. Caso não exista controle interno em determinado departamento da empresa, a auditoria interna deve recomendar sua implantação, visando maior segurança na manutenção e geração das informações.

Para a análise dos riscos operacionais e da qualidade dos controles internos existentes, a auditoria interna deve aplicar os modelos COSO e COBIT, principalmente, nas organizações que pretendem manter relações econômicas com países estrangeiros, uma vez que auxiliam as organizações quanto às exigências da Lei Sarbanes-Oxley (SOX).

Segundo artigo publicado por Sandonato (2007):

“O Framework COSO, o mais utilizado para governança corporativa e gerenciamento de riscos, foi lançado em 2003, e o comitê responsável por sua implantação também implantou o conceito de Enterprise Risk Management Framework (ERM).”

Com relação ao COBIT, estrutura de controles internos sobre gestão dos recursos de tecnologia da informação, Sandonato (2007) comenta: “Por ser um modelo reconhecido, abrangente e independente de plataformas tecnológicas, o COBIT tornou-se uma referência para a conformidade da TI com a SOX”. Sandonato (2007) apresenta assim a estrutura COSO e COBIT (Figura 2):

“Criados a partir de boas práticas, estas estruturas integram as informações dos principais processos organizacionais, sob a forma “cubos”, a partir do qual os diversos pontos de controle são aplicados nas diversas dimensões da organização, no caso do COSO, e dos recursos de tecnologia da informação, no caso do COBIT”.

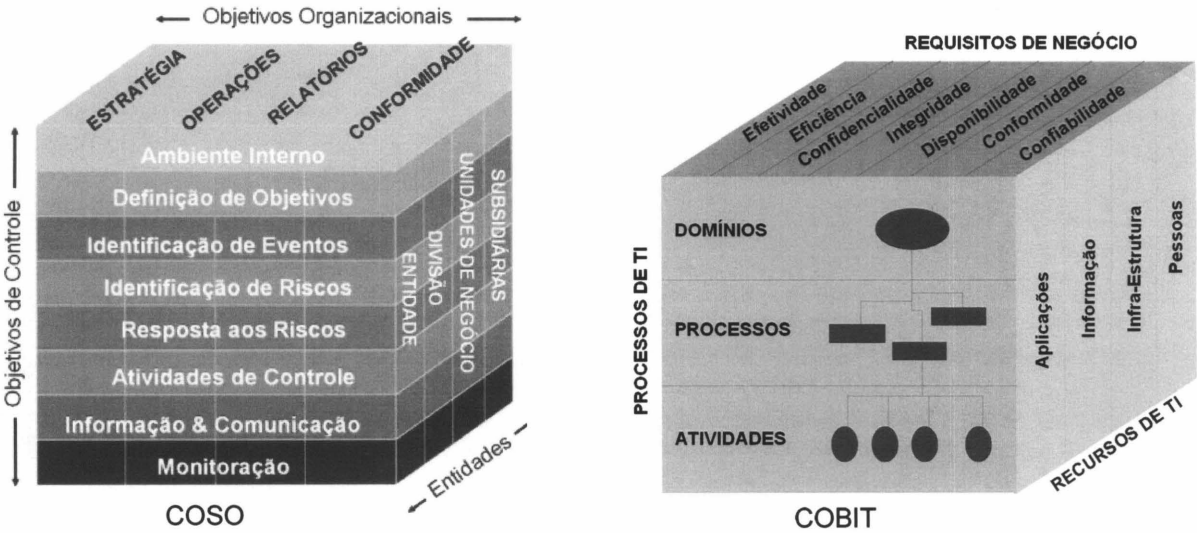


Figura 2 - Metodologias COSO e COBIT
Fonte: Sandonato, 2007

3.1 Self Assessment (CSA)

Conforme *The Institute of Internal Auditors - IIA* (AUDIBRA, 2009, p. 6):

“CSA é um processo através do qual as efetividades dos controles internos são examinadas e avaliadas. O objetivo é prover razoável segurança de que todos os objetivos do negócio serão alcançados.”

Baseia-se no conhecimento adquirido no dia-a-dia e minimiza a busca de evidências, provas e análises. Pode ser apresentado em forma de *workshops*, questionários e auto-análise gerencial. Os mais utilizados são os questionários -

que devem conter periodicidade de aplicação, perguntas claras e concisas, instruções completas em relação à amostragem e revisão atualizada e a auto-análise gerencial – que contém questionários desenvolvidos pela gerência para suportar as avaliações dos controles e o cumprimento dos regulamentos, além de investigação interna sobre fraudes ou falhas. Fatores importantes para o sucesso do CSA (*Ibid*, p. 10) são: a cultura organizacional, o apoio da alta administração, o envolvimento dos gerentes e *staff* e a implementação das medidas corretivas.

Na Figura 3 apresenta a abrangência alcançada pelo CSA se comparado a outras metodologias de controle.



Figura 3 – Ampliação do “espectro” de controles
Fonte: AUDIBRA, 2009, p.21

Comparando a metodologia utilizada pelo CSA com a auditoria tradicional encontramos:

Quadro 2 – Quadro comparativo Auditoria x CSA

<u>AUDITORIA TRADICIONAL</u>	<u>CSA</u>
AVALIAÇÃO DE CONTROLES	
<ul style="list-style-type: none"> • Responsabilidade de controle pré-estabelecida • Participação limitada das equipes • Auditores são os únicos especialistas em controles 	<ul style="list-style-type: none"> • Controle é responsabilidade de todos • Participação ampla das equipes • Especialização em controle é compartilhada em todos os níveis
RESPONSABILIDADES DAS GERÊNCIAS E EQUIPES	
<ul style="list-style-type: none"> • Devem seguir/executar os controles • Escassos treinamentos sobre controles para as equipes • Quem realiza a atividade não é responsável pelo controle • Medo e culpa 	<ul style="list-style-type: none"> • Desenho e manutenção dos controles • As equipes são capacitadas em controles • Discussão franca e aberta em todos os níveis
OBJETIVOS DA AUDITORIA	
<ul style="list-style-type: none"> • Realizar as auditorias e relatar “pontos” • Recomendações 	<ul style="list-style-type: none"> • Elevar as habilidades das equipes de avaliar e desenhar controles • Feedback mais objetivo • Os auditores instruem, treinam e facilitam as equipes

Fonte: AUDIBRA, 2009, p. 23

Enquanto a auditoria interna despende tempo com pesquisas preliminares, avaliações das estruturas de controles, auditorias operacionais e as áreas operacionais de baixo risco, o CSA complementa o ambiente de controle, a avaliação de riscos e eficiência dos controles, comunicação e monitoramento.

3.2 COSO

Em 1985, foi criada, nos Estados Unidos, a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis. Esta comissão era composta por representantes das principais associações de classe de profissionais ligados à área financeira e seu primeiro objeto de estudo foram os controles internos. Em 1992 publicaram o trabalho "*Internal Control - Integrated Framework*" (Controles Internos - Um Modelo Integrado). Esta publicação tornou-se referência mundial para o estudo e aplicação dos controles internos. Posteriormente a Comissão transformou-se em Comitê, que passou a ser conhecido como COSO - *The Committee of Sponsoring Organizations* (Comitê das Organizações Patrocinadoras).

A metodologia adotada pelo COSO (AUDIBRA; PricewaterhouseCoopers, 2007), parte do princípio que existe um relacionamento direto entre os objetivos a serem alcançados pela organização e os componentes de gerenciamento de risco, que representam o que é necessário para alcançar tais objetivos. Sua representação é uma matriz tridimensional em forma de cubo (Figura 2). As quatro categorias de objetivos estão representadas nas colunas verticais. Os componentes de controle, em um total de 8 itens, estão nas linhas horizontais e as unidades da organização na terceira dimensão.

Conforme o COSO (*Ibid*, p. 7): "Essa representação ilustra a capacidade de manter o enfoque na totalidade do gerenciamento de riscos de uma organização, ou na categoria de objetivos, componentes, unidade da organização ou qualquer um dos subconjuntos." Esta metodologia não tem como meta substituir as estruturas de controles internos existentes nas organizações, mas aprimorar seu conteúdo de maneira que sirva de base para um processo mais amplo de gerenciamento de riscos.

O COSO (*Ibid*, p. 3), apresenta assim as finalidades do gerenciamento de riscos corporativos:

- **Alinhar o apetite a risco com a estratégia adotada** – os administradores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos.

- **Fortalecer as decisões em resposta aos riscos** – o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos – como evitar, reduzir, compartilhar e aceitar os riscos.
- **Reduzir as surpresas e prejuízos operacionais** – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados.
- **Identificar e administrar riscos múltiplos e entre empreendimentos** – toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos inter relacionados e, também, respostas integradas aos diversos riscos.
- **Aproveitar oportunidades** – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa.
- **Otimizar o capital** – a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

O gerenciamento de riscos corporativos trata de riscos e oportunidades que afetam a preservação dos ativos. É um processo contínuo que flui através da organização, conduzido por todos os profissionais em todos os níveis, deve ser aplicado à definição das estratégias e inclui a formação de uma visão de portfólio de todos os riscos a que a organização está exposta.

A avaliação de riscos de uma organização inclui uma combinação de técnicas qualitativas e quantitativas. A técnica qualitativa se aplica quando os riscos não podem ser quantificados ou se não há dados confiáveis em quantidade suficiente para a realização das avaliações quantitativas, ou se a relação custo-benefício para obtenção e análise dos dados não for viável.

“Tipicamente, as técnicas quantitativas emprestam maior precisão e são utilizadas em atividades mais complexas e sofisticadas para complementar as técnicas qualitativas. As técnicas quantitativas de avaliação geralmente requerem mais esforço e rigor, muitas vezes utilizando modelos matemáticos não triviais. As técnicas quantitativas dependem sobremaneira da qualidade dos dados e das premissas adotadas e são mais relevantes para exposições que apresentem um histórico conhecido, uma frequência de sua variabilidade e permitam uma previsão confiável.” (Ibid, p. 50)

Exemplos de técnicas quantitativas estão apresentadas no Quadro 3:

Quadro 3 – Técnicas quantitativas de avaliação de riscos

<p>Comparação com Referências de Mercado (Benchmarking) – É um processo cooperativo entre um grupo de organizações. O benchmarking enfoca eventos ou processos específicos, compara medições e resultados utilizando métricas comuns, bem como identifica oportunidades de melhoria. Dados de eventos, processos e medidas são desenvolvidos para a comparação de desempenho. Algumas Companhias utilizam o benchmarking para avaliar a probabilidade e o impacto de eventos em potencial em uma indústria.</p> <p>Modelos Probabilísticos – Os modelos probabilísticos associam a uma gama de eventos e seu respectivo impacto, a probabilidade de ocorrência sob determinadas premissas. A probabilidade e o impacto são avaliados com base em dados históricos ou resultados simulados que refletem hipóteses de comportamento futuro. Os exemplos de modelos probabilísticos incluem valor em risco (value-at-risk), fluxo de caixa em risco, receitas em risco e</p>	<p>distribuição de prejuízo operacional e de crédito. Os modelos probabilísticos podem ser utilizados com diferentes horizontes de tempo para estimar os seus resultados, como a faixa de prazos dos instrumentos financeiros disponíveis. Os modelos probabilísticos também podem ser usados para avaliar resultados esperados ou médios em relação a impactos imprevistos ou extremos.</p> <p>Modelos Não Probabilísticos – Os modelos não probabilísticos empregam critérios subjetivos para estimar o impacto de eventos, sem quantificar uma probabilidade associada. A avaliação do impacto de eventos baseia-se em dados históricos ou simulados a partir de hipóteses sobre o comportamento futuro. Os exemplos de modelos não probabilísticos incluem medições de sensibilidade, testes de estresse e análises de cenários.</p>
---	---

Fonte: AUDIBRA; PricewaterhouseCoopers, 2007, p. 57

A estrutura de gerenciamento de riscos corporativos apresentada pelo COSO (*Ibid*, p. 5), está classificada em quatro categorias:

- **Estratégicos** – metas gerais alinhadas com a missão da organização
- **Operações** – utilização eficaz e eficiente dos recursos
- **Comunicação** – confiabilidade nos relatórios
- **Conformidade** – cumprimento de leis e regulamentos aplicáveis

Os componentes de gerenciamento de risco corporativos, conforme o COSO (*Ibid*, p. 22), é constituído de oito itens inter-relacionados e se originam na maneira como a

administração gerencia a organização e se integram ao processo de gestão. São eles:

- **Ambiente Interno** – refere-se à filosofia quanto ao tratamento dos riscos e quais os limites estabelecidos. Determinam os conceitos básicos sobre a forma de como os riscos e os controles serão abordados pelos empregados da organização. Envolve atributos individuais dos colaboradores como: integridade, valores éticos e competência.
- **Fixação de Objetivos** – Assegura que a administração adote um processo para estabelecer objetivos que propiciem suporte à missão da organização e estejam compatíveis com o apetite a risco.
- **Identificação de Eventos** – Os eventos gerados por fontes internas ou externas afetam a realização dos objetivos e devem ser identificados. Podem ser diferenciados em riscos, oportunidades ou ambos. As oportunidades devem ser canalizadas à administração para definição das estratégias.
- **Avaliação de Riscos** – Sua finalidade é determinar a forma como serão administrados os riscos identificados e quais objetivos podem ser influenciados. Os riscos são avaliados considerando seus efeitos inerentes e residuais, bem como sua probabilidade e seu impacto.
- **Resposta a Risco** – Possíveis respostas ao risco, identificadas pelos colaboradores: evitar, aceitar, reduzir ou compartilhar. As ações destinadas a alinhar os riscos às respectivas tolerâncias e ao apetite ao risco são de responsabilidade da administração.
- **Atividades de Controle** – Implementação e estabelecimento de políticas e procedimentos que assegurem que as respostas aos riscos selecionados pela administração sejam executadas com eficácia.
- **Informações e Comunicações** – A eficácia da comunicação ocorre quando esta flui em todas as direções na organização e quando os colaboradores recebem informações claras e precisas quanto às suas funções e responsabilidade.
- **Monitoramento** – Atividades de gerenciamento contínuas e avaliações independentes são rotinas de monitoramento e permitem que a organização reaja ativamente e modifique suas ações conforme as circunstâncias.

Ao agrupar e categorizar os eventos, a administração consegue identificar oportunidades e riscos com maior facilidade.

Em COSO (*Ibid*, p. 50), encontramos:

“Ao agregar os eventos horizontalmente em uma organização e verticalmente nas unidades operacionais, a administração desenvolverá a compreensão do relacionamento entre os eventos e poderá adquirir melhores informações para formar uma base para avaliar riscos.”

A classificação dos eventos pode ter como base, a própria classificação de objetivos da organização, iniciando-se nos objetivos gerais até chegar aos objetivos correlatos às unidades ou funções organizacionais ou processos. O Quadro 4 apresenta uma abordagem utilizada dentro do contexto de fatores mais amplos internos e externos.

Quadro 4 – Categorias de Eventos

Fatores Externos	Fatores Internos
<u>Econômicos</u> Disponibilidade de capital Emissões de crédito, inadimplência Concentração Liquidez Mercados financeiros Desemprego Concorrência Fusões / aquisições	<u>Infra-estrutura</u> Disponibilidade de bens Capacidade dos bens Acesso ao capital Complexidade
<u>Meio Ambiente</u> Emissões e dejetos Energia Desastres naturais Desenvolvimento sustentável	<u>Pessoal</u> Capacidade dos empregados Atividade fraudulenta Saúde e segurança
<u>Políticos</u> Mudanças de governo Legislação Plítica pública Regulamentos	<u>Processo</u> Capacidade Design Execução Dependência / fornecedores
<u>Sociais</u> Características demográficas Comportamento do consumidor Cidadania corporativa Privacidade Terrorismo	<u>Tecnologia</u> Integridade de dados Disponibilidade de dados e sistemas Seleção de sistemas Desenvolvimento Alocação Manutenção
<u>Tecnológicos</u> Interrupções Comércio eletrônico Dados externos Tecnologias emergentes	

3.3 COBIT

O *IT Governance Institute* (ITGI) foi estabelecido em 1998 com o intuito de melhorar o pensamento e os padrões internacionais de direção e controle da tecnologia da informação organizacional. O ITGI oferece pesquisa, recursos eletrônicos e estudos de caso para o auxílio aos líderes das organizações e ao conselho de diretores na responsabilidade de governança de TI.

Conforme o ITGI (2007, p. 7 e 11):

“A governança de TI é de responsabilidade dos executivos da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. (...) Sua missão é pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação.”

Para tanto, as organizações devem satisfazer requisitos de qualidade, guarda e segurança de suas informações.

O *Control Objectives for Information and related Technology* (COBIT), através de um modelo de domínios e processos, fornece boas práticas que ajudam a otimizar os investimentos em TI, assegurar a entrega de serviços e prover métricas para julgar quando existem erros. Para obtenção de sucesso, O COBIT:

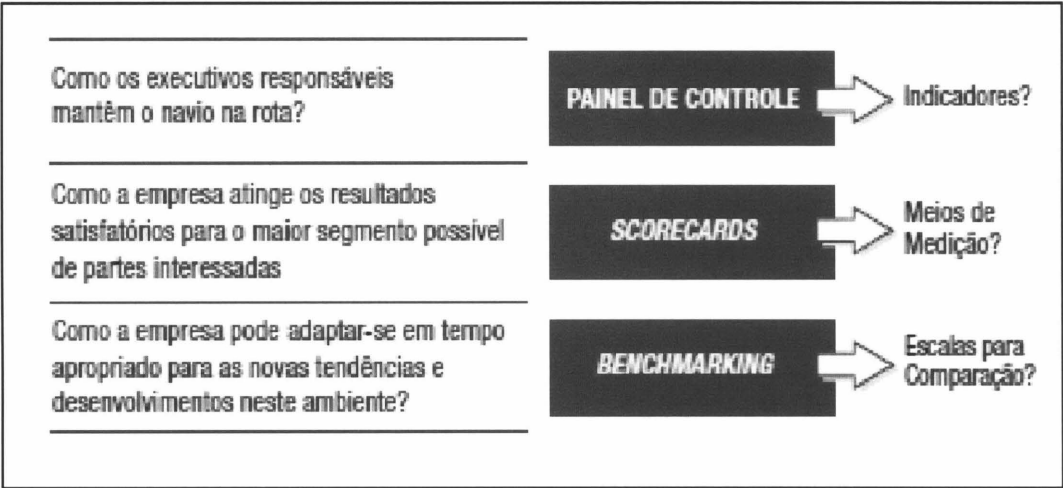
- Faz a ligação com os requisitos de negócios;
- Organiza as atividades de TI em um modelo de processos geralmente aceitos;
- Identifica os mais importantes recursos de TI a serem utilizados;
- Define os objetivos de controle gerenciais a serem considerados.

Para O ITGI:

“O foco em processos do COBIT é utilizado por um modelo de processos de TI subdivididos em quatro domínios e 34 processos em linha com as áreas responsáveis por planejar, construir, executar e monitorar, provendo assim uma visão total da área de TI. Conceitos de arquitetura corporativa ajudam a identificar os recursos essenciais para o sucesso dos processos, ou seja, aplicativos, informações, infra-estrutura e pessoas.” (Ibid, p. 7)

O quadro a seguir apresenta algumas questões e ferramentas que auxiliam as organizações nas suas necessidades de melhoria.

Quadro 5 – Gerenciamento de Informações



Fonte: ITGI, 2007, p. 7

O COBIT influencia diferentes usuários (*Ibid*, p. 27):

- **Alta Direção** – para obter valor dos investimentos de TI balancear os riscos e controlar o investimento em um ambiente de TI às vezes imprevisível.
- **Executivos de negócios** – para assegurar que o gerenciamento e o controle dos serviços de TI oferecidos internamente e por terceiros estejam funcionando de modo adequado.
- **Executivo de TI** – para prover os serviços de TI de que o negócio precisa para suportar a estratégia de negócios de maneira controlada e gerenciada.
- **Auditores** – para substanciar suas opiniões e/ou prover recomendações sobre controles internos para os executivos.

As áreas de foco da governança de TI são descritas em alguns tópicos que auxiliam os executivos no direcionamento (Quadro 6).

Quadro 6 – Áreas de Foco na Governança de TI



- Alinhamento estratégico: foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização.
- Entrega de valor: é a execução da proposta de valor de TI através do ciclo de entrega, garantindo que a TI entregue os prometidos benefícios previstos na estratégia da organização, concentrando-se em otimizar custos e provendo o valor intrínseco de TI.
- Gestão de recursos: refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem-se à otimização do conhecimento e infraestrutura.
- Gestão de risco: requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite da empresa e dos requerimentos de conformidade, transparência sobre os riscos significativos para a organização e inserção do gerenciamento de riscos nas atividades da companhia.
- Mensuração de desempenho: acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de performance e entrega dos serviços, usando, por exemplo, “*balance scorecards*” que traduzem as estratégias em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

Fonte: ITGI, 2007, p. 8

Os componentes do COBIT são inter-relacionados e proporcionam o suporte necessário à governança, gerenciamento, controle e avaliação, conforme Figura 4.

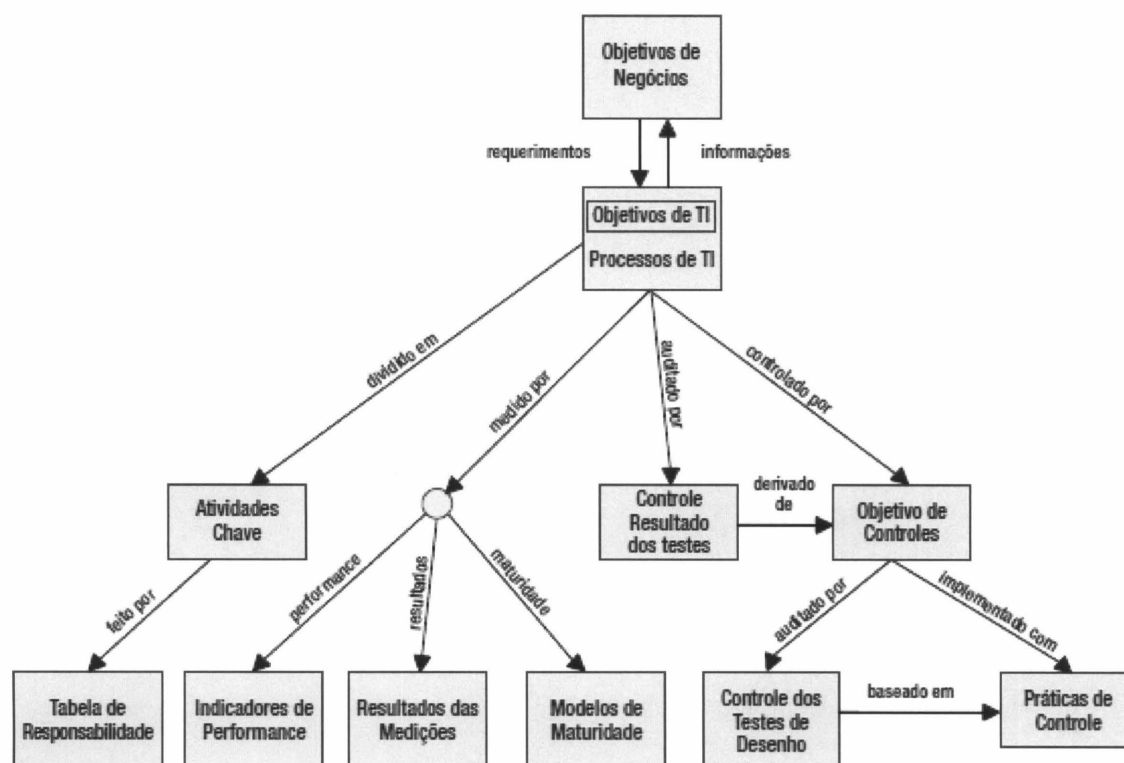


Figura 4 – Inter-relacionamento dos componentes COBIT

Fonte: ITGI, 2007, p. 10

Os benefícios de implementação do COBIT incluem:

- Melhor alinhamento com o foco do negócio;
- Visão mais clara para os executivos sobre o que a TI faz;
- Melhor apresentação da divisão de responsabilidades baseada na orientação para processos;
- Aceitação por terceiros e órgão reguladores;
- Cumprimento dos requisitos do COSO para controle de ambiente de TI.

Os critérios de informação fornecem um método genérico para definição dos requisitos e objetivos do negócio, enquanto os critérios de TI fornecem uma base mais refinada para o estabelecimento dos requisitos e desenvolvimento de métricas que permitam avaliar se os objetivos foram alcançados.

Conforme o ITGI (Ibid, p. 13):

“Para a área de TI entregar de maneira bem-sucedida os serviços que suportam as estratégias de negócios, deve existir uma clara definição das responsabilidades e direcionamento dos requisitos pela área de negócios (o cliente) e um claro entendimento acerca do que e como precisa ser entregue pela TI (o fornecedor).”

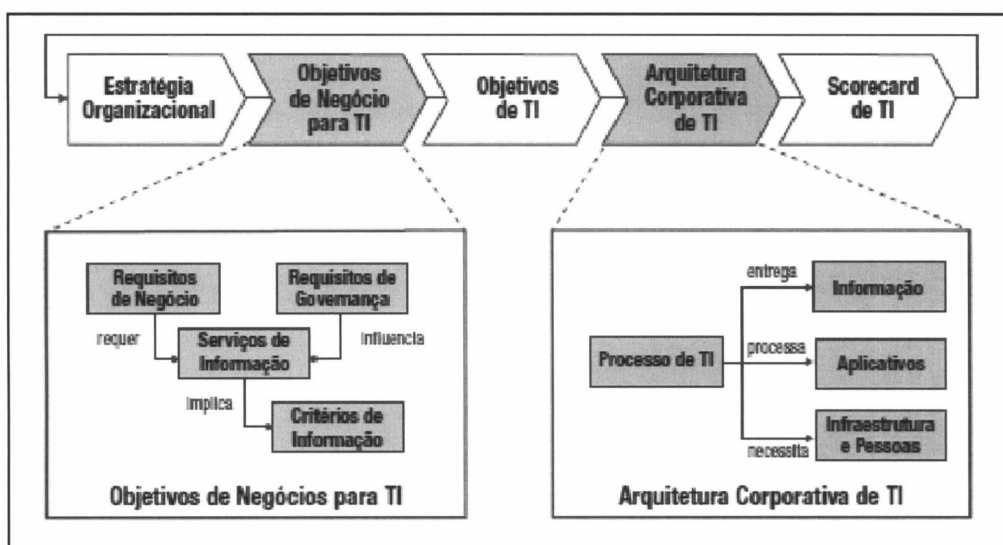


Figura 5 – Definindo os Objetivos de TI e a Arquitetura da Empresa para TI
 Fonte: ITGI, 2007, p. 13

A Figura 5 apresenta a definição dos objetivos próprios da área de TI (os objetivos de TI) que por sua vez definem os recursos e capacidades de TI (a arquitetura de TI para a organização) necessários para a execução da parte que cabe à TI na estratégia da empresa, de maneira bem-sucedida.

4 AUDITORIA INTERNA E A GOVERNANÇA CORPORATIVA

Segundo o Instituto Brasileiro de Governança Corporativa - IBGC (2009, p. 19):

“Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade.”

Independente de seu porte ou natureza jurídica, os princípios e práticas da boa Governança Corporativa, aplicam-se a qualquer tipo de organização.

A Figura 6 apresenta o que seria uma estrutura organizacional ideal para o sistema de Governança Corporativa.

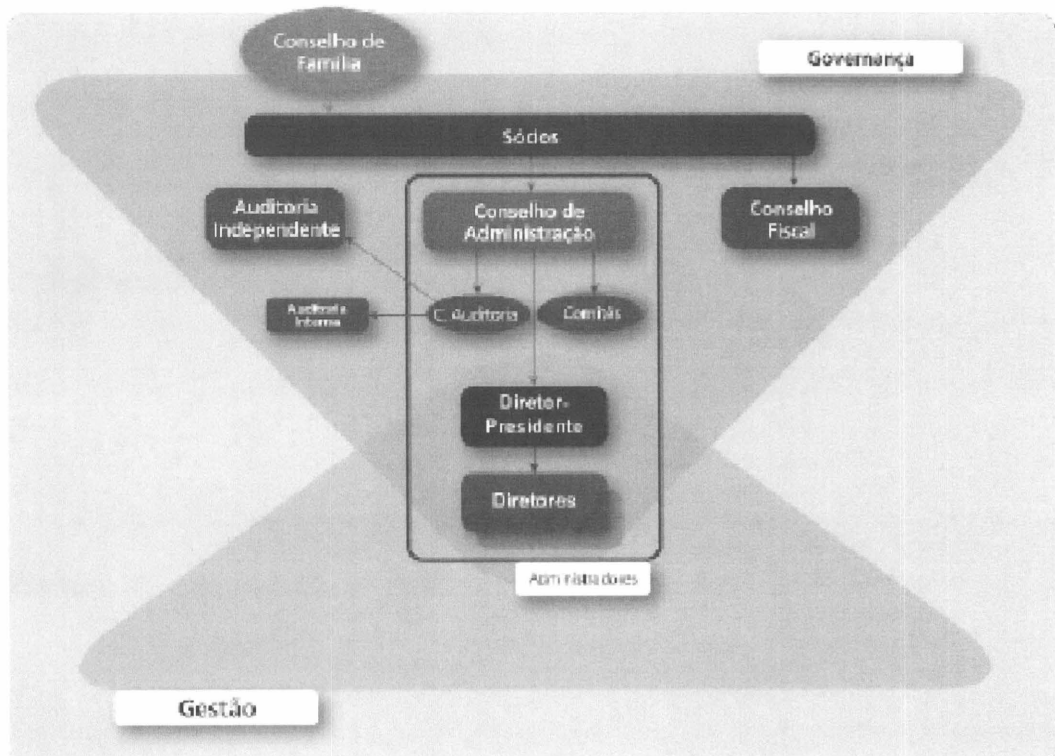


Figura 6 – Sistema de Governança Corporativa
Fonte: IBGC, 2009, p. 16

Os princípios básicos da Governança Corporativa, segundo o IBGC, são (*Ibid*, p. 19):

- **Transparência** – Disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas as impostas por disposições de leis ou regulamentos. Não se restringe ao desempenho econômico-financeiro, mas contempla também demais fatores que norteiam as ações gerenciais e que conduzem a criação de valor.
- **Equidade** – Tratamento justo para todos os sócios e demais partes interessadas (stakeholders). É totalmente inaceitável qualquer tipo de atitude ou política discriminatória, sob qualquer pretexto.
- **Prestação de Contas (accountability)** – Os agentes de governança devem prestar contas de sua atuação, assumindo integralmente as consequências de seus atos e omissões.
- **Responsabilidade Corporativa** – Os agentes de governança devem zelar pela sustentabilidade das organizações, objetivando sua longevidade, incorporando considerações de ordem social e ambiental na definição dos negócios e operações.

O gerenciamento dos riscos corporativos está assim definido pelo IBGC:

“O Conselho de Administração deve assegurar-se de que a Diretoria identifica preventivamente – por meio de um sistema de informações adequado – e lista os principais riscos aos quais a organização está exposta, além da sua probabilidade de ocorrência, a exposição financeira consolidada a esses riscos (considerando sua probabilidade de ocorrência, o impacto financeiro potencial e os aspectos intangíveis) e as medidas e os procedimentos adotados para sua prevenção ou mitigação. (*Ibid*, p. 31)

O IBGC recomenda a instituição do Comitê de Auditoria para:

- Analisar as demonstrações financeiras;
- Promover a supervisão e responsabilidade da área Financeira;
- Garantir o desenvolvimento de controles internos confiáveis;
- Garantir que a Auditoria Interna desempenhe a contento o seu papel e que os auditores independentes avaliem, por meio de sua própria revisão, as práticas da Diretoria e da Auditoria Interna;
- Zelar pelo cumprimento do Código de Conduta da organização.

Cabe aos Auditores Internos atuar proativamente na recomendação do aperfeiçoamento dos controles, das normas e dos procedimentos. Sua atuação ativa beneficia a gestão da organização e, principalmente, ao diretor-presidente. Para tanto, seu trabalho deve estar perfeitamente alinhado com a estratégia da organização.

Quanto ao relacionamento com a Auditoria Interna, o IBGC recomenda:

“A Auditoria Interna deve reportar-se ao Comitê de Auditoria ou, na falta deste, ao Conselho de Administração. Nas empresas em que não houver Conselho de Administração, a Auditoria Interna deve reportar-se aos sócios, de forma a garantir independência em relação à gestão.” (Ibid, p. 49)

Embora se reporte ao Comitê de Auditoria ou ao Conselho de Administração, a Auditoria interna deve ouvir as demandas de melhoria de ambientes de controles vindas da gestão.

5 IMPLANTANDO A ÁREA DE AUDITORIA INTERNA

Conforme as melhores práticas de mercado, utilizadas pelas *Big Four* da Auditoria no Brasil, a implantação da Auditoria Interna em uma organização, demanda tempo, conhecimento do negócio e esforços da alta direção no sentido de buscarem a melhoria nos processos de governança corporativa. A implantação da função de auditoria interna envolve custos elevados em treinamento de pessoal e manutenção da qualidade do trabalho. Por isso, a contratação de serviço especializado, no primeiro momento, pode reduzir o custo da implantação e garantir a utilização e a atualização das ferramentas necessárias.

Baseada em uma proposta de implantação de Auditoria Interna, temos a seguir uma visão mais ampla dos processos com enfoque em gestão de riscos dos processos.

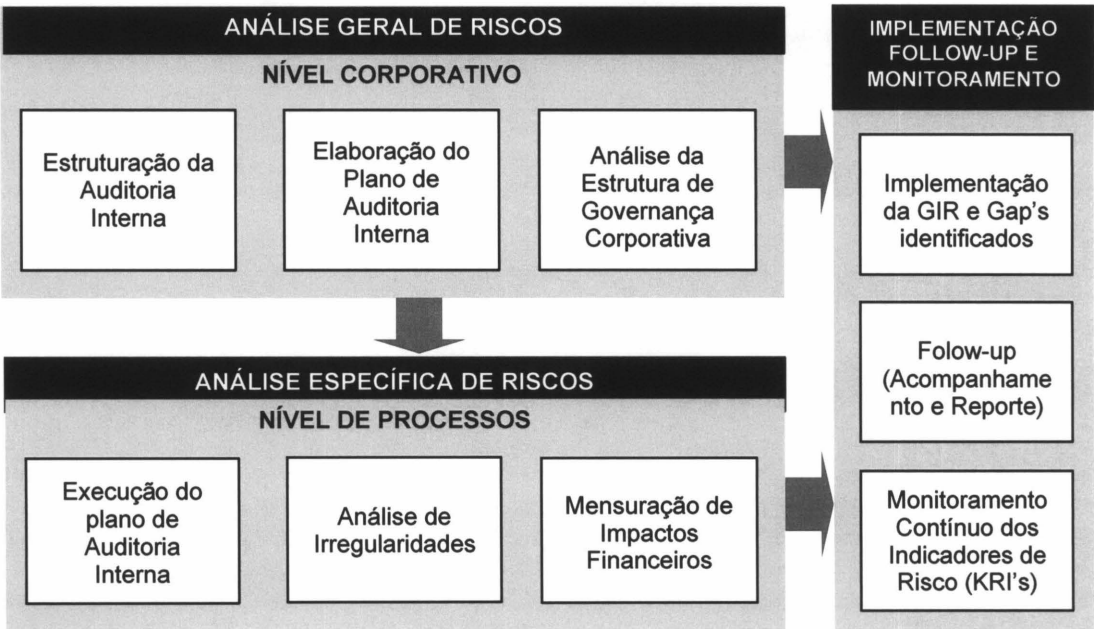


Figura 7 – Enfoque de Trabalho

Entretanto, por ser um processo longo e oneroso, e por ter como objetivo a focalização e priorização dos riscos relevantes, as organizações optam por priorizarem as seguintes etapas:

- Estruturação da Auditoria Interna
- Elaboração do Plano de Auditoria Interna
- Execução do Plano de Auditoria Interna

5.1 Estruturação da Auditoria Interna

Como principais atividades na estruturação da Auditoria Interna, destacam-se:

- Entendimento da cultura de controles, riscos e auditoria interna existentes;
- Inventário de todas as necessidades existentes (ou futuras) que atendam as exigências relativas à estrutura organizacional para estar em compliance com o que a companhia deseja;
- Mapeamento da estrutura organizacional existente, o que já atende a essas expectativas e o que não, a fim de criar ou adaptar a estrutura para atender aos órgãos (Bovespa e SEC) e objetivos da companhia;
- Definição conjunta de componentes da infra-estrutura que melhor endereça a realidade e objetivos, considerando: Política de Auditoria Interna; Definição do Processo de Auditoria Interna; Estrutura Organizacional; Subordinação e níveis de reporte; Funções e Responsabilidades; Metodologia e Enfoque de Atuação; Relacionamento com demais áreas de negócio.

As empresas de auditoria entendem que o bom relacionamento existente entre as áreas da organização (Figura 8) e a definição de suas atribuições é fator importante para alçar o sucesso quando da implantação da Auditoria Interna. Podemos citar como exemplos de atribuições para cada área:

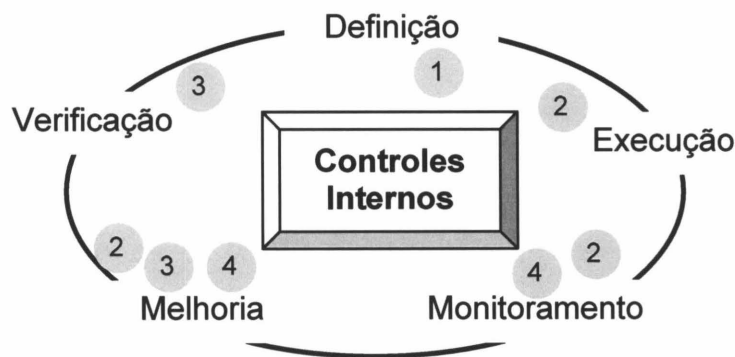


Figura 8 – Relacionamento entre as Áreas da Organização

Onde:

1 – Alta Administração

- Elabora as estratégias de negócio;
- Define diretrizes gerais (políticas) e limites de exposição ao risco;

- Fornece os recursos necessários;
- Responsável final pelo adequado funcionamento do ambiente de controles.

2 – Áreas de Negócio

- Executa as ações;
- Monitora as operações no dia-a-dia;
- Assume riscos;
- Implementa os controles.

3 – Auditoria Interna

- Realiza trabalhos de revisão de aspectos operacionais e financeiros, assim como das funções de gestão de riscos;
- Fornece uma avaliação independente do ambiente de controles internos;
- Auxilia a organização a melhorar seus processos de negócio.

4 – Gestão de Riscos

- Define metodologias para mensuração e sistemática de acompanhamento;
- Consolida os resultados e comunica para a Alta Administração;
- Identifica riscos inerentes às operações;
- Conduz processo de auto-avaliação e acompanha as operações de forma independente;
- Avalia o grau de exposição.

5.2 Elaboração do Plano de Auditoria Interna

Para a elaboração do Plano de Auditoria, são recomendadas as seguintes ações:

- Entendimento da organização considerando principais segmentos de atuação, processos de negócios e respectivas atividades;
- Desenvolvimento de questionário para entendimento dos principais riscos da organização;
- Condução de entrevistas com os principais executivos, identificando os principais riscos associados aos processos/áreas críticas de negócio;

- Consolidação das percepções quanto à exposição aos riscos, conforme resultado das entrevistas com os principais executivos;
- Priorização dos processos de negócio com base na percepção de riscos dos principais executivos;
- Elaboração de um plano de Auditoria Interna com base nos principais riscos e processos priorizados.

A identificação dos riscos é etapa importante para a elaboração do Plano de Auditoria Interna, uma vez que permitem priorizar os processos, definido assim as ações mais imediatas na mitigação dos riscos apresentados. Para a identificação dos riscos é necessário conhecer os processos e sub-processos da organização para uma análise criteriosa dos efeitos destes no resultado da mesma.

Os riscos a serem analisados podem ser classificados em:

- Estratégicos
- Operacionais
- Financeiros
- Regulamentares

Enquanto que o resultado deve sempre gerar valores aos acionistas, como por exemplo:

- Aumento da receita;
- Otimização dos custos operacionais;
- Eficiência dos ativos;
- Atendimento das expectativas.

Após identificação dos riscos, as melhores práticas de controle devem ser avaliadas para o processo, através de *benchmarking*, e efetuados os testes para validação, ou não, dos controles existentes e sua eficácia. De posse dos resultados das análises dos riscos, seus controles e abrangência, monta-se o mapa de risco da organização. Por não existir um padrão para sua apresentação, aplicam-se as melhores práticas de mercado utilizadas pelas maiores empresas de Auditoria, onde o risco é classificado em alto, médio e baixo, conforme sua criticidade.

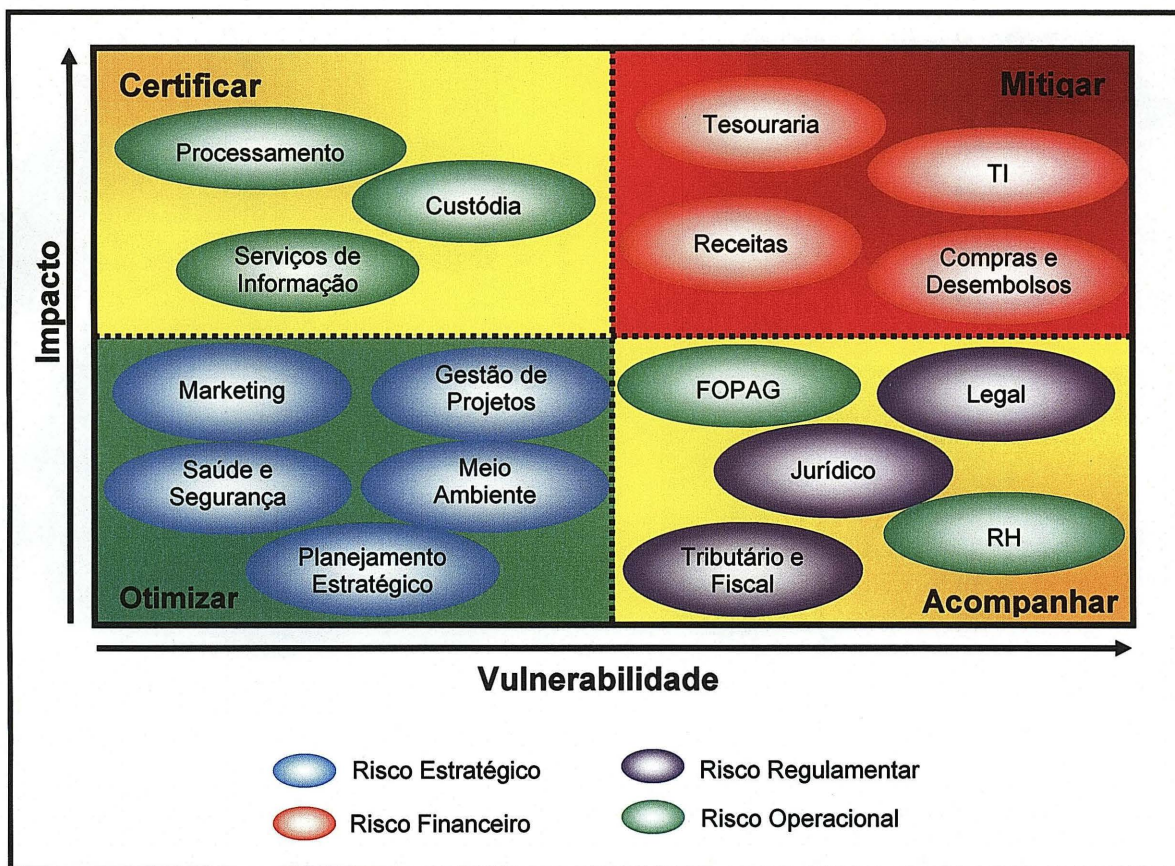


Figura 9 – Mapa de Riscos

A Figura 9 apresenta um exemplo de mapa de risco onde estão alocados alguns processos analisados. O resultado deste mapeamento será a base do Programa de Auditoria.

Os quadrantes coloridos indicam o grau de criticidade do processo e a consequente urgência de revisão do mesmo. Quanto ao grau de criticidade, podemos dizer:

- Quadrante vermelho – o risco é alto e, independente da existência ou não de controles, precisa ser acompanhado;
- Quadrante amarelo – o risco é médio e os controles, ou não existem, ou não se mostraram eficazes;
- Quadrante verde – o risco é baixo e pode ou não existir controles de mitigação. Durante a priorização dos processos pelos gestores, estes serão os últimos a serem tratados.

O Plano de Auditoria Interna pode ser assim apresentado:

Quadro 7 – Plano de Auditoria Interna

Processo	Primeiro Ano											
	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Tesouraria												
TI												
Receitas												
Compras e Desembolsos												
Processo	Segundo Ano											
	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Tesouraria												
TI												
Receitas												
Compras e Desembolsos												
Custódia, Processamento e Serviços de Informação												
RH / FOPAG												
Jurídico, Legal e Regulatório												
Processo	Terceiro Ano											
	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Tesouraria												
TI												
Receitas												
Compras e Desembolsos												
Planejamento Estratégico e Marketing												
Gestão de Projetos												
Meio Ambiente, Saúde e Segurança												

5.3 Execução do Plano de Auditoria Interna

De posse do Plano de Auditoria a área já possui orientação suficiente para dar início aos trabalhos indicados. A área deve atentar aos prazos estipulados e a quantidade de testes necessários. Diferentemente da Auditoria Externa que trabalha por amostragem, a Auditoria Interna efetua seus testes em todas as execuções de determinado processo, existentes em um período pré-determinado. Caso os resultados não sejam satisfatórios ou deixem margem a dúvidas, testes complementares se fazem necessários, mesmo que sobre um mesmo tema.

A Auditoria Interna, para realização de seus trabalhos, utiliza-se dos mesmos papéis de trabalho do Auditor Externo. Devido à quantidade de documentos movimentados quando da realização da auditoria, apenas aqueles relacionados aos processos

considerados inadequados devem ser arquivados, para futura consulta ou como justificativa para as recomendações realizadas.

Findo o trabalho de auditoria e implementação dos *Gap's* identificados, rotinas de *follow-up* e monitoramento dos processos já auditados devem ser instituídas, permitindo um melhor acompanhamento quanto ao cumprimento das recomendações apresentadas no Relatório da Auditoria. A adoção destas rotinas também facilita a compreensão, por parte da Alta Administração, da situação encontrada à época da auditoria e a atual, bem como os efeitos e reflexos gerados.

A periodicidade de uma auditoria em determinado processo, está diretamente relacionado a dois fatores: sua relevância e criticidade dentro do ambiente operacional da organização, verificado através do trabalho de auditoria; e a visão da Alta Administração quanto à segurança e execução de determinado processo.

6 CONCLUSÃO

Quando se fala em implantação da área de Auditoria Interna nas empresas, a primeira imagem que vem à cabeça dos componentes da organização é a figura do “dedo-duro”. Aquele que irá passar os dias procurando erros e apontando culpados. Na realidade a função de auditor interno é exatamente o oposto. Seu trabalho consiste em analisar, avaliar e sugerir melhorias nos processos existentes ou implantação dos inexistentes, a fim de permitir que a organização alcance os objetivos traçados pela Alta Administração. Esta, por sua vez, ao tomar decisões de ordem estratégica para a manutenção e o crescimento do negócio, necessita de garantias formais de que tanto os resultados financeiros quanto a operação da organização estão se realizando de maneira satisfatória. Estas garantias formais estão presentes nos pareceres dos Auditores Externos (Independentes) que validam a veracidade dos números apresentados pela Contabilidade, enquanto que a Auditoria Interna garante o cumprimento das metas e objetivos da organização.

A existência da área de Auditoria Interna nas organizações também se faz necessária quando se trata de atender as boas práticas de Governança Corporativa, muito exigidas pela CVM (Comissão de Valores Mobiliários) e a SEC (*Securities and Exchange Commission*), órgão norte-americano responsável pela implantação da SOX (lei Sarbanes-Oxley). Apesar de a Governança Corporativa estar intimamente ligada às empresas que negociam suas ações no mercado, sua prática deve ser adotada por todas as empresas que têm como objetivo maior transparência nos seus negócios.

Sendo assim, a utilização de ferramentas como o COSO, o COBIT e o Self Assessment (CSA), bem como, a adoção de controles internos eficazes que suportem as normas institucionais e os processos operacionais existentes, permitem ao Auditor Interno que seu trabalho esteja de acordo com as melhores práticas de mercado. O monitoramento constante destes processos e os riscos originários inerentes à operação da organização estejam sob controle e não sejam perdidos de vista, garantindo a continuidade da organização e a sustentação para as tomadas de decisão. Além de garantir aos fornecedores externos que as informações e práticas divulgadas estão de acordo com as normas legais, institucionais e de mercado.

REFERÊNCIAS

ALMEIDA Marcelo Cavalcante. **Auditoria: um curso moderno e completo**. 6. ed. São Paulo: Atlas, 2003.

GIL, Antonio de Loureiro. **Auditoria de Negócios – Auditoria Governamental – Contingências versus Qualidade**. 2. ed. São Paulo: Atlas, 2002.

IMONIANA, Joshua Onome. **Auditoria – Abordagem Contemporânea**. São Paulo: J. O. Imoniana, 2001.

SANDONATO, Franco dos Santos. **A importância dos frameworks de controle de processos para a gestão efetiva da tecnologia**. In: XXVII Encontro Nacional de Engenharia – ENEGEP, 2007, Foz do Iguaçu. Disponível em: <http://www.abepro.org.br/biblioteca/ENEGEP2007_TR630468_0476.pdf>. Acesso em 18/01/2010.

SEMINÁRIO DE AUDITORIA INTERNA – AUDIBRA, 2009, Vitória. Disponível em: <[http://www.audibra.org.br/seminarios/2009/03vitoria/4_Guilherme_Machado_Control%20Self%20Assessment%20\(CSA\)%20Intensificando%20os%20Controles.pdf](http://www.audibra.org.br/seminarios/2009/03vitoria/4_Guilherme_Machado_Control%20Self%20Assessment%20(CSA)%20Intensificando%20os%20Controles.pdf)>. Acesso em: 20/01/2010

PORTAL DA EDUCAÇÃO. Disponível em: <<http://www.portaleducacao.com.br/gestao-e-lideranca/artigos/6304/diferencas-basicas-entre-a-auditoria-interna-e-a-auditoria-externa>>. Acesso em 18/01/2010.

Instituto dos Auditores Internos do Brasil – AUDIBRA; PricewaterhouseCoopers. **COSO – Gerenciamento de Riscos Corporativos – Estrutura Integrada**. São Paulo, 2007. Disponível em: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em 18/01/2010.

IT Governance Institute - ITGI™. COBIT 4.1. 2007

Instituto Brasileiro de Governança Corporativa – IBGC. **Código das Melhores Práticas de Governança Corporativa**. São Paulo, 2009. Disponível em: <<http://www.ibgc.org.br/CodigoMelhoresPraticas.aspx>>. Acesso em 18/01/2010.